In the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method for scanning and cleaning computer viruses, comprising the steps of:

simulating in a computer a virtual computer circumstance [[~~that~~]] on which the computer viruses reside;

providing a plurality of objects or baits to be infected [[-]] by computer viruses [[~~for inducing~~]] that induce virus infection;

loading a target object to be scanned into said simulated virtual computer circumstance;

activating the target object to be scanned in said simulated virtual computer circumstance to induce the computer viruses possibly attached on said target object to infect the plurality of objects to be infected and generating standard samples which have been infected;

comparing the plurality of objects after processing in the activating step with the plurality of objects to be infected originally provided, and determining whether there is any change or not; [[~~, if yes,~~]] if there is a change then the target object to be scanned contains a virus, otherwise the target object to be scanned is free of [[~~virus~~]] viruses;

analyzing and learning from the viruses by analyzing the generated standard samples and extracting information and knowledge on the viruses indicated by changes between the standard samples before infection and after infection when it is determined that said target object to be scanned contains a virus; and

cleaning viruses from the infected target object by removing the virus's body and modifying key information which has been changed by said virus on the basis of said information and knowledge on the viruses indicated by changes between the standard samples before infection and after infection and on the basis of the modification at viruses have made to said infected objects or baits.

2. (Cancelled)

3. (Previously presented) The method according to claim 1, wherein said computer simulation step includes providing functional functions to call and execute the steps of:

simulating a Central Processing Unit (CPU) by simulating instructions of the CPU;

simulating an Operating System (OS) by simulating various services and various data structures provided by the OS;

simulating peripheral storage devices by simulating storage space and structures of various peripheral storage devices including simulated hard disk and floppy disk and the like; and

simulating a memory by generating, distributing and managing a simulated memory space.

4. (Currently amended) The method according to claim 3, wherein said provided objects to be infected includes [[~~all kinds of~~]] baits that have different sizes and contents for inducing viruses of different types and [[~~various~~]] infection conditions, [[~~, such as, baits of DOS files type for files of DOS COM type to induce viruses of DOS COM type, simulated DOS boot sector for inducing viruses of DOS boot sector type, baits of WORD files type for inducing viruses of macro viruses, and so on.~~]]

5. (Currently amended) The method according to claim 4, wherein a plurality of baits having different sizes and contents are provided for a given virus type to satisfy the infection conditions of the viruses attached in the target object to be scanned [[~~as possible as they can~~]].

6. (Original) The method according to claim 5, further comprising the step of simulating the system time to generate virtual system date and time for inducing the viruses that are sensitive to date and time.

7. (Original) The method according to claim 6, wherein said simulating OS includes simulating one of operating systems DOS, WINDOWS, and UNIX.

8. (Currently amended) The method according to claim [[~~2~~]] 1, wherein in the step of virus cleaning, the virus is virtually ran to restore the original target object from the infected host object, i.e. the target object to be scanned that had been judged to be carrying virus, thus the virus is cleaned.

9. (Currently amended) The method according to claim 3, wherein in the step of simulating the peripheral storage device, a [[~~small~~]] memory space is assigned in the memory to simulate a virtual hard disk [[~~, which has the same structure as a normal one,~~]] including three-dimension space by sector number, track number and cylinder number, a primary boot sector and corresponding blank sector of the No. 0 track, and next boot sector, File Allocation Table, root directory sector, necessary system files, and bait files for inducing viruses.

10. (Currently amended) The method according to claim 3, wherein in the step of simulating the peripheral storage device, a [[~~small~~]] memory space is assigned in the memory to simulate a virtual floppy disk [[~~, which has the same structure as a normal one,~~]] including boot sector, a File Allocation Table, a root directory sector, necessary system files, and bait files for inducing viruses, [[~~etc.~~]]

11. (Currently amended) A computer system including a general computer for scanning and cleaning computer viruses, comprising:

a computer simulation unit for simulating in the computer a virtual computer circumstance [[~~that~~]] on which the computer viruses resides;

a plurality of objects or baits to be infected by computer viruses [[~~for inducing~~]] that induce virus infection;

a control unit for loading a target object to be scanned into said simulated virtual computer circumstance;

a virus infection inducing unit for activating the target object to be scanned in said simulated virtual computer circumstance to induce the computer viruses possibly attached on said target object to infect the plurality of objects to be infected and generating standard samples which have been infected;

a virus decision unit for comparing the plurality of objects after processing in virus infection inducing unit with the plurality of objects to be infected originally provided, determining whether there is any change or not; [[~~, if yes,~~]] if there is a change then the target object to be scanned contains a virus, otherwise the target object to be scanned is free of viruses;

a virus analyzing and learning means for analyzing the generated standard samples and extracting information and knowledge on the viruses indicated by changes between the standard samples before infection and after infection when it is judged at there is virus; and

a virus cleaning unit for cleaning viruses from the infected target object to be scanned by removing virus's body and modifying key information which has been changed by said virus according to said information and knowledge on the viruses indicated by changes between the standard samples before infection and after infection and the basis of the modification that viruses have done to said infected objects or baits.

12. (Cancelled)

13. (Previously presented) The system according to claim 11, wherein said computer simulation it includes:

a Central Processing Unit (CPU) simulation unit for simulating instructions of the CPU;

an Operating System (OS) simulation unit for simulating various services and various data structures provided by the OS;

a peripheral storage device simulation unit for simulating storage space and structures of various peripheral storage devices including simulated hard disk, floppy disk and the like; and

a memory simulation unit for generating, distributing and managing a simulated memory space, wherein said respective units include functional functions available to be called and allocated memory space, and are independent from specific CPU, OS, and peripheral storage devices.

14. (Currently amended) The system according to claim 13, wherein said provided objects to be infected includes [[~~all kinds of~~]] baits that have different sizes and contents for inducing viruses of different types and [[~~various~~]] infection conditions. [[~~, such as, baits of DOS~~

~~files type for files of DOS COM type to induce viruses of DOS COM type, simulated DOS boot sector for inducing viruses of DOS boot sector type, baits of WORD files type for inducing viruses of macro viruses, and so on.~~]]

15. (Currently amended) The system according to claim 14, wherein a plurality of baits having different sizes and contents are provided for a given virus type to satisfy the infection conditions of the viruses attached in the target object to be scanned. [[~~as possible as they can.~~]]

16. (Original) The system according to claim 15, further comprises a system time simulation unit for generating virtual system date and time to induce the viruses that are sensitive to date and time.

17. (Original) The system according to claim 16, wherein said OS simulation simulates one of the plurality operating systems DOS, WINDOWS, and UNIX.

18. (Original) The system according to claim 12, wherein said virus cleaning unit run the virus to restore the original target object from the infected host object, i.e. the target object to be scanned that had been judged to be carrying [[a]] virus, thus the virus is cleaned.

19. (Currently amended) The system according to claim 13, wherein said peripheral storage devices simulation unit assigns a [[~~small~~]] memory space in the memory to simulate a virtual hard disk [[~~, which has the same structure as a normal one,~~]] including three-dimension space by sector number, track number and cylinder number, a primary boot sector and corresponding blank sector of the No. 0 track, and next boot sector, File Allocation Table, root directory sector, necessary system files, and bait files for inducing viruses.

20. (Currently amended) The system according to claim 13, wherein said peripheral storage devices simulation unit assigns a [[~~small~~]] memory space in the memory to simulate a virtual floppy disk [[~~, which has the same structure as a normal one,~~]] including a boot sector, a

File Allocation Table, a root directory sector, necessary system files, and bait files for inducing viruses, [[~~etc.~~]]

21. (Previously presented) A computer readable recording medium for causing a computer to execute the steps of the method described in claim 1.

22. (Currently amended) A transmission medium for causing a computer to execute the steps of the method described in claim 1 via network transmission.